

# Exhibit 1

January 2011

## Traffic Report: Online Piracy and Counterfeiting

## Traffic Report: Online Piracy and Counterfeiting

---

### Contents

Key Findings .....	4
Methodology .....	4
Criteria for Websites .....	5
Traffic Analysis .....	7
Conclusion .....	8

The Internet is arguably one of the greatest innovations of modern society—allowing for countless new businesses to thrive and dramatically altering the way society operates. The Internet has enabled a global marketplace to flourish with lightning-quick communication and an unparalleled access to information. However, the advancement of the Internet into nearly all of our daily activities, combined with rapid download speeds, the perfection of digital copies, the rise of e-commerce and the complexity of online enforcement, has magnified the seriousness and consequences of online counterfeiting and piracy. Websites offering pirated goods generate billions of visits annually, and websites that sell counterfeit luxury goods, fake drugs, and products that may pose health and safety risks attract hundreds of millions annually.

Recognizing that illicit online sales have a significant impact on the U.S. economy in financial terms as well as in public health and well-being, MarkMonitor® worked to identify a sample of rogue Internet sites that are responsible for trafficking counterfeit and pirated goods. The goal of the project was to illustrate the nature of this illicit ecosystem and, using publicly-available traffic information on the number of visits, determine its scope.

The first step was to identify business categories and brands targeted by online counterfeiters and digital pirates. Using 22 major brands as criteria—ranging from pharmaceuticals, luxury goods, and apparel to entertainment titles and software—MarkMonitor used its patented technology to comb the Internet for sites suspected of offering counterfeit goods or pirated digital content. The initial scans resulted in more than 10,000 results which were then de-duplicated and filtered further using MarkMonitor technology to identify dedicated e-commerce and digital download sites. The final step required hand-examination and verification of more than 600 results to determine classification. Since some sites offered multiple brands, this step led to almost 100 unique domains or websites which were then classified in one of two ways: ‘counterfeit’ or ‘digital piracy’.

Using publicly-available Internet traffic data from Alexa, the sites were then ranked by the number of visits, which were significant, speaking to the level of demand for these goods as well as to the website operators’ success in promoting these sites so they are visible and accessible online. Since the study used a sample of only 22 brands, it provides a small glimpse of the nature of online intellectual property (IP) theft and the dark side of illicit e-commerce. However, given the large number of popular brands, it is reasonable to assume that hundreds of thousands of other rights-holders, brands and content creators are suffering the same damage.

---

*“As our economy  
has worsened,  
brand abusers have  
sharpened their focus.”*

## Key Findings

The study's findings demonstrate that online distribution of pirated digital content and e-commerce sales of counterfeit goods is rampant. Specific findings include:

- In total, the 10 media brands in the study yielded 43 unique sites classified as 'digital piracy.' Traffic generated to these sites was over 146 million visits per day, representing more than 53 billion visits per year.
- The top-three websites classified as 'digital piracy'—rapidshare.com, megavideo.com, and megaupload.com—collectively generate more than 21 billion visits per year.
- The availability of reliable infrastructure is an important factor in the location of sites hosting piracy. The study found that North America and Western Europe represented the host location for 67 percent of the sites classified as 'digital piracy.'
- The combined traffic to the 48 sites selling counterfeit goods is more than 240,000 visits per day on average or more than 87 million visits per year.
- When it comes to host location of the sites categorized as 'counterfeit', 73 percent were hosted in North America or Western Europe. Eastern European countries hosted another 14 percent of the sites while 9 percent of the sites were hosted in Asia.
- The combined traffic to the 26 sites selling counterfeit prescription drugs is more than 141,000 visits per day on average or more than 51 million visits per year.
- The combined traffic to the 21 e-commerce sites selling counterfeit luxury goods is more than 98,000 visits per day on average or almost 36 million visits per year.

These findings are just the tip of the iceberg. The true scope of the problem is exponentially higher in terms of user traffic, lost revenue and risks to public health and safety.

## Methodology

Using a list of industries most affected by online counterfeiting and digital piracy,<sup>1</sup> MarkMonitor chose major brands from each industry and ran automated scans for those brands using its patented technology. In all, the study examined 22 brands in the digital content category (movies/TV shows, music and software/videogames) and the physical goods category (handbags, sports apparel, pharmaceuticals and luxury items, footwear, and apparel.)

The study used very narrow criteria to classify sites selling physical goods as 'counterfeit.' It is important to point out that many of the e-commerce sites that did not meet that strict guideline did display multiple factors arousing suspicion. This

---

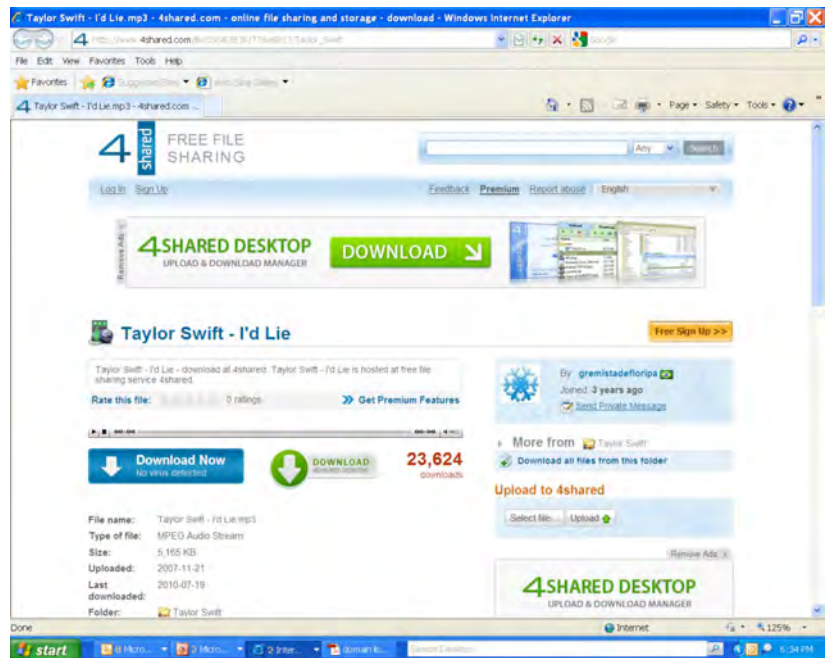
*“The study used only 22 brands, so we can assume that many other brands and content-creators are suffering similar damage.”*

---

<sup>1</sup> Digital Content industries: Entertainment (music/movies/television shows), Software/Videogames; Physical Goods: Handbags, Sports Apparel with logos, Pharmaceuticals, luxury items, footwear, and apparel.

underscores the crucial role that brand owners and law enforcement personnel trained by brand owners play in determining whether a site is offering counterfeit goods. Technology can be used to conduct the heavy lifting in identifying and prioritizing sites for further action, but the in-depth market and product knowledge of brand owners' is vital.

The scans focused on identifying e-commerce and peer-to-peer, streaming, and torrent sites that yielded high traffic levels. In order to be classified as an e-commerce site, the site needed to contain a shopping cart while the sites classified as piracy needed to contain some type of link, index or player that could be used to download, stream or share digital content. These criteria were designed to eliminate editorial, blog or discussion sites and to focus exclusively on sites where pirated goods could be shared, viewed, streamed or downloaded and counterfeit goods could be purchased.



Site attracts more than 10 million visits per day.

The initial scans resulted in more than 10,000 results which were then de-duplicated and filtered further using MarkMonitor technology to identify dedicated e-commerce and digital content sites used for downloading, sharing or streaming. The final step required hand-examination and verification of more than 600 results to determine classification. Since some sites offered multiple brands, this step led to almost 100 unique domains or websites which were then classified as either 'counterfeit' or 'digital piracy'. The results were ranked by the amount of traffic, defined as the number of daily visits, using Alexa-supplied information. None of the scans contained MarkMonitor customer data or information.

## Criteria for Websites

The results from the initial scans were examined further by MarkMonitor experts in order to classify these sites, or domains, into one of two categories: 'counterfeit' or 'digital piracy.' After thorough analysis, MarkMonitor concluded that 91 websites with high traffic numbers qualified for inclusion in one of these categories. The 'counterfeit' classification referred to e-commerce sites selling counterfeit physical goods while the 'digital piracy' classification refers to sites offering pirated versions of music, movies, television shows, software, and videogames.

**Digital Piracy:** The total number of unique domains identified as 'digital piracy' totaled 43. To fit the 'digital piracy' classification, the domain needed to offer or point to one or more of the brands used in the digital content portion of the study for free. While some of these sites do offer takedown processes for pirated

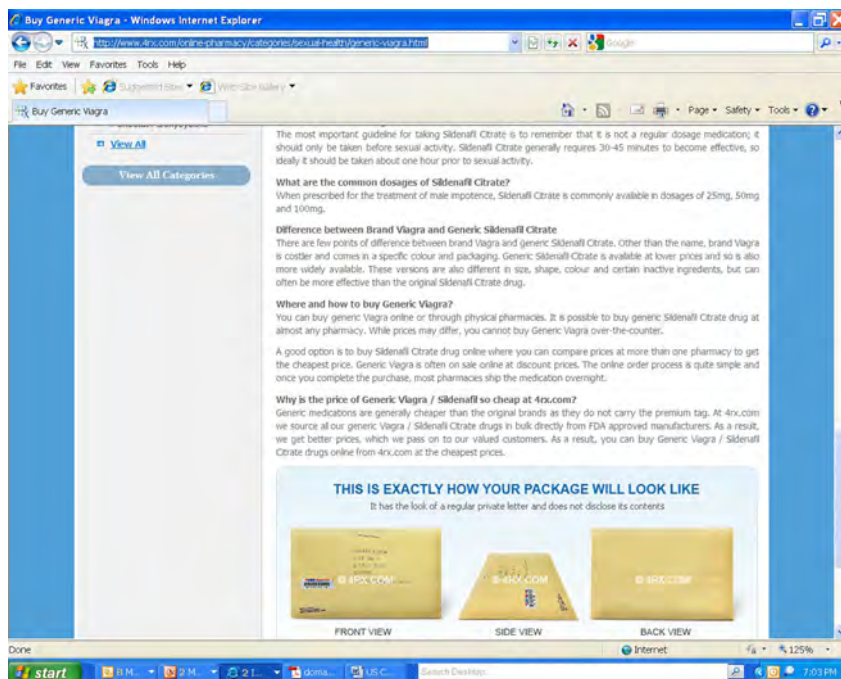
content, the action must be initiated by the content owner. The resulting domains were then sorted by traffic volume.

**'Counterfeit':** In the case of e-commerce domains selling physical goods, the domains needed to satisfy one of two conditions to be deemed as selling counterfeit goods: (1) either the domain itself specified that the goods were not authentic (i.e., using terms like 'replica,' 'knock-off,' and 'copy') or (2) in the case of pharmaceuticals, the domain offered 'generic' versions of prescription drugs that are not available in generic form in the U.S., targeted the U.S. market by providing pricing in U.S. currency, and did not require a prescription.<sup>2</sup> Since some domains offered more than one type of product, the domain is counted only once, even if multiple URLs for that domain surfaced during the scans. MarkMonitor found that 48 websites fell under the criteria for selling counterfeit goods.

While the online pharmacies displayed the 'generic' label prominently on product listings, MarkMonitor needed to consult FAQ or 'About' sections of the online drugstores, or even needed to follow the purchase process, in order to determine if prescriptions were required by the online pharmacy. In addition, MarkMonitor examined the currency used to quote prices, shipping information or other information on the site that indicated markets served, such as flags, shipping information, telephone numbers or references to the U.S. Drug Enforcement Agency. Many of the e-commerce domains selling counterfeit goods displayed the term 'replica' quite prominently while others included such information in their FAQ or 'About.'



Site sells 'generics' without prescription for prescription drugs that are not available in generic form.



Site explains the difference between 'generic' and branded prescription drugs and highlights unmarked shipping envelopes.

<sup>2</sup> During the course of the study, MarkMonitor identified some additional sites that fit the criteria for inclusion but did not use one of the original media brands such as sites offering key generators used to 'unlock' protected material.



## Traffic Analysis

As a backdrop to examining website traffic figures, it is important to point out that traffic measurements can vary greatly depending on methodology. Some traffic measurement sources depend on technology, others depend on some type of user panel or community, and a third category uses a hybrid approach. Each approach has advantages and disadvantages which, as a result, allow publicly-available traffic data to vary based upon the measurement source. In this study, MarkMonitor used data based on Alexa. The more than 90 unique domains culled from the initial set of over 10,000 results display a wide range of traffic figures, depending on the type of goods being offered.

**Digital Piracy Web Traffic Analysis:** Those domains classified as ‘digital piracy’ attracted the highest levels of traffic with a high in excess of 32 million daily visits on average for the most-trafficked domain—rapidshare.com. On an annual basis, that traffic equates to more than 11.8 billion visits per year for that site. This pattern continues with the second and third most-trafficked sites—megavideo.com and megaupload.com—each of which generates more than 13 million visits per day on average, or more than 4.9 billion visits per year to each site. Collectively, these three digital piracy sites generate more than 21 billion visits per year.

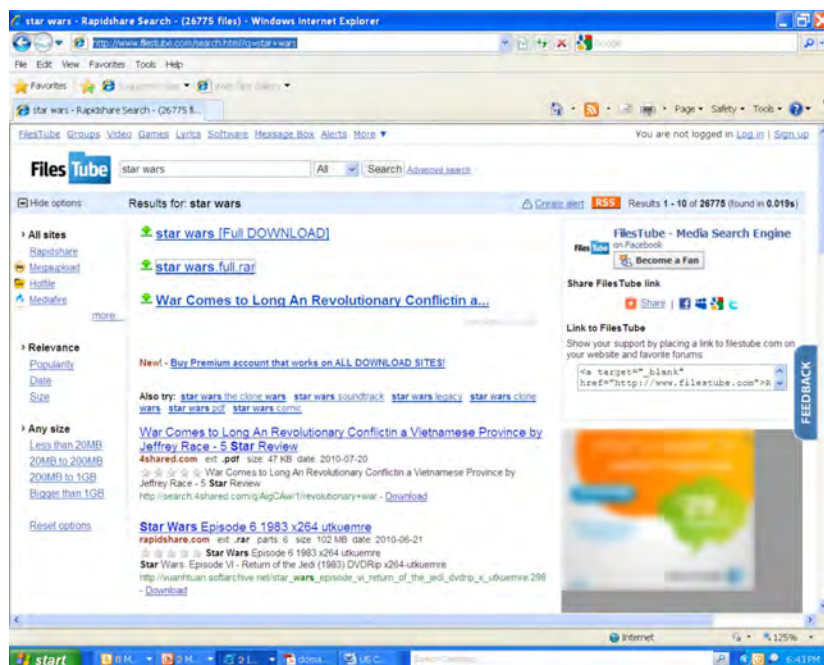
In total, traffic generated to the sites classified as ‘digital piracy’ was more than 146 million visits per day, representing more than 53 billion visits per year. Lest these figures be viewed as anomalies, examining the ten least-visited ‘digital piracy’ sites show annual visits total more than 781 million per year, demonstrating that even the lesser-trafficked sites in this category drive significant traffic.

The bulk of the ‘digital piracy’ sites, or 67 percent, were hosted in North America or Western Europe.

**Counterfeit Website Traffic Analysis:** Due to the narrow criteria used to classify sites

as ‘counterfeit,’ all the sites included in the analysis, with one exception, sold prescription drugs or luxury goods, including handbags, watches or jewelry. The combined traffic to the 48 sites selling counterfeit goods is more than 240,000 visits per day on average or more than 87 million visits per year. The majority of these sites reflect similar patterns as the sites classified as ‘digital piracy’ when it comes to the server’s host location with or 56 percent hosted in North America and Western Europe. However, Eastern European countries hosted 22 percent of the sites while 14 percent of the sites were hosted in Asia.

*“Traffic to sites suspected of offering pirated content was over 146 million visits per day.”*



Site attracts more than seven million visits per day.



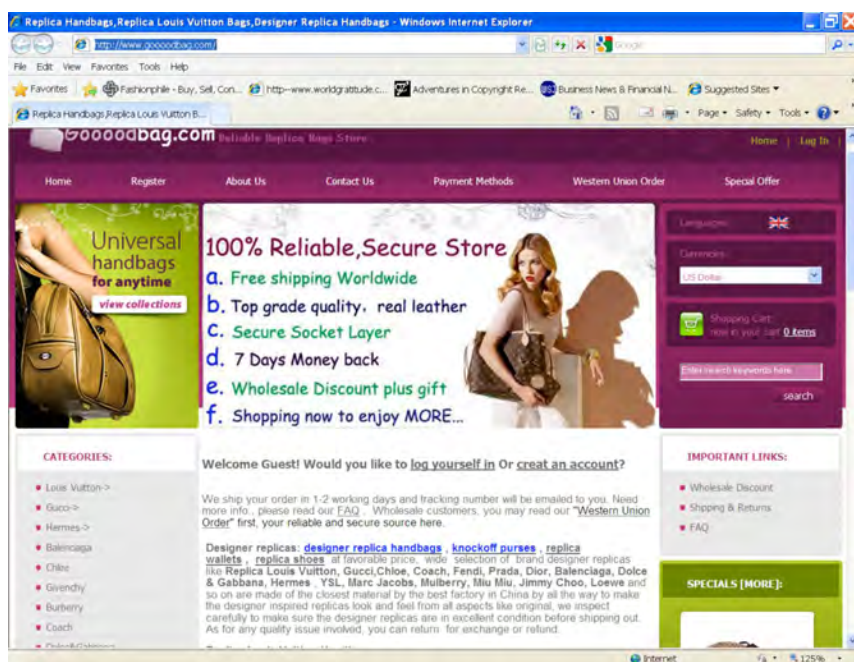
However, examining the site registration information for these ‘counterfeit’ sites suggests that more of these sites may be linked to Asia as seven sites hosted in non-Asian countries are actually registered by Asian registrars. Factoring in that information indicates that 29 percent of the sites have some connection to Asia, either through host location or registrar.

While not at the scale of the suspected digital piracy sites, e-commerce domains classified as ‘counterfeit’ attracted considerable levels of traffic as well with the most-trafficked site, an Internet pharmacy, driving 28,000 daily visits on average, representing more than 10 million visits to the site per year.

**Suspicious Sites:** During the course of the research, we identified sites that displayed one or more factors that appeared questionable, such as significant price discounts, links to sites selling counterfeit goods, trade dress issues, or, in the case of online pharmacies, no requirement for prescriptions. These types of issues underscore the crucial role that brand owners and law enforcement personnel trained by brand owners play in determining whether a site is offering counterfeit or pirated goods. While some sites are very clear in specifying their goods are ‘copies’ or ‘replicas,’ others are less forthcoming. In many cases, deep discounts combined with promises of high-quality goods from the current season raise questions that only the brand owner—with knowledge of channel strategy, pricing and partnerships—can address.

In the case of highly regulated goods like pharmaceuticals, intellectual property protections for pharmaceutical patents or regulations governing generics may differ across national boundaries. Instead, the business practices of the pharmacy itself—such as prescription requirements or sales of individual pills—are more useful in identifying suspicious drugs. The role of the brand owner, with in-depth knowledge of distribution channels, pricing and local business practices, is vital. In each of these examples, the most authoritative answer is provided by a physical examination of the goods themselves.

*“Combined traffic to the sites selling counterfeit goods is more than 87 million visits per year.”*



This site promotes replica designer bags and attracts more than two million visits annually.

## Conclusion

The research presented in this study demonstrates the wide availability of pirated digital content and counterfeit goods via the Internet and e-commerce. The websites yielded in the research and analyses of this study all have one thing in common: business models that are indisputably centered on the sale or distribution of counterfeit and pirated goods. These illegal operations are shifting revenue

from legitimate brands' e-commerce sites, causing economic harm and risking consumer health. This study highlights the type of data that needs to be examined in order to identify and locate sites trafficking in counterfeit and pirated goods. Accurate and unbiased information describing the scope of online counterfeiting and piracy as an essential prerequisite for safeguarding consumer safety and economic well-being.

While counterfeiting and piracy in the physical world are serious problems, these issues are growing at a significant rate online and pose unique challenges in remediation, due to the inherent nature of the Internet with its global reach, cost efficiencies, and anonymity. Awareness and educational efforts focused on the distinctive nature of online counterfeiting and piracy are necessary in developing effective response mechanisms to this global, cross-border problem. Necessary government policies, corrective legislative measures, law enforcement action and, most importantly, actively-engaged brand owners are all needed to stem this growing tide of illegal Internet activity. The bottom line is that online IP theft ultimately affects the most creative and innovative sectors of the economy, contributing to billions in lost revenue and millions of lost jobs. Protecting IP rights is a critical component of our economic resurgence, and vitally important to our future; stopping the spread of pirated and counterfeit goods is a necessity.

---

*“Combined traffic to the pharmacies selling suspected counterfeit prescription drugs is more than 51 million visits per year.”*

## About MarkMonitor

MarkMonitor, the global leader in enterprise brand protection, offers comprehensive solutions and services that safeguard brands, reputation and revenue from online risks. With end-to-end solutions that address the growing threats of online fraud, brand abuse and unauthorized channels, MarkMonitor enables a secure Internet for businesses and their customers. The company's exclusive access to data combined with its patented real-time prevention, detection and response capabilities provide wide-ranging protection to the ever-changing online risks faced by brands today. For more information, visit [www.markmonitor.com](http://www.markmonitor.com)

More than half the Fortune  
100 trust MarkMonitor to  
protect their brands online.  
**See what we can do for you.**

MarkMonitor, Inc.  
U.S. (800) 745.9229  
Europe +44 (0) 207.840.1300  
[www.markmonitor.com](http://www.markmonitor.com)

## White Paper

# Seven Best Practices for Fighting Counterfeit Sales Online

## Executive Summary

Counterfeit sales represent 5 to 7 percent of world merchandise trade today<sup>1</sup>. The damage these sales do to rightful brand owners goes well beyond revenues and profits: numerous reports have suggested that counterfeit and piracy trade supports terrorism, organized crime and other threats to both national security and human rights. Now, the Internet's rapid growth—along with its instant global reach and anonymity—has significantly escalated the situation.

An entire online supply chain, parallel to legitimate distribution channels, has flourished around counterfeit goods. Online B2B exchanges, in addition to eCommerce sites—many promoted via social media and search engines—commonly traffic in counterfeit goods. Fake products acquired on wholesale sites are sold on auction sites, or at flea markets and shops in the physical world.

Deceptive use of proven marketing techniques—paid search ads, search engine optimization, unsolicited email, the use of branded terms in domain names and more—are important parts of this illicit ecosystem, as savvy counterfeiters apply marketing best practices.

Fortunately, brand owners can adopt their own proven best practices to successfully combat online counterfeit sales. Technology exists for identifying and quantifying worldwide online counterfeiting activity—in both promotion and distribution—as it affects a specific brand. Once visible, infringement can be prioritized and attacked. Unlike anti-counterfeiting strategies in the physical world, however, a two-pronged approach is necessary: brand owners must choke off counterfeit sales at both promotional and distribution points.

The battle against online counterfeit sales can be won. With billions in revenues, critical customer loyalty, and even public safety and human rights at stake, it must.

## Contents

Counterfeiting: A Growing Online Threat .....	3
Counterfeiting's Real Cost to Business .....	3
How Counterfeiting Thrives Online .....	4
Beating Back Counterfeiters Online: Seven Best Practices .....	5
Conclusion: The Fight Is Yours to Win .....	9

## Counterfeiting: A Growing Online Threat

“If you can make it, you can fake it.” Unfortunately, the old saying is all too true. Sales of counterfeit goods affect a wide range of industries, from high-margin luxury and technology goods to low-margin consumer goods like batteries, shampoo, gasoline and food.

The problem is growing, in part because the volume of fake goods produced is rapidly increasing—especially in countries like China, where manufacturing capacities continue to skyrocket (89 percent of seized counterfeit products originate there).<sup>2</sup>

This growth in supply helps fuel the exploding demand—especially online. The Internet’s rapid growth—along with its instant global reach and anonymity—has significantly escalated the situation, moving the sale of counterfeit goods from the local street corner to a global marketplace. Because criminals can quickly and easily set up eCommerce storefronts or place listings on B2B exchanges and on auction sites—with only minor expense—their activities will likely cost legitimate businesses \$135 billion in lost revenue this year.

## Counterfeiting’s Real Cost to Business

According to the secretary general of the ICC, multinational manufacturers lose roughly ten percent of their top-line revenue to counterfeiters<sup>3</sup>—but the impacts go well beyond the revenue hit. For some companies, perceived brand value suffers when knock-offs become plentiful. Brands may even lose representation in distribution channels when resellers and affiliates see a reduction in demand due to competition from fakes. Additionally, the availability of cheaper, albeit fake alternatives can exert downward pressure on legitimate brand pricing.

Other impacts include product safety issues—especially in pharmaceutical, automotive, aviation, healthcare electronics and similar industries—accompanied by increased legal liability risks. And as consumers experience quality problems with fake goods, the legitimate brand’s customer service and warranty costs can climb.

Marketing costs also rise as illicit sellers bid up paid search advertising costs and erode legitimate search engine optimization (SEO) investments. Finally, as more customers encounter inauthentic brand experiences, both loyalty and lifetime customer value suffer.

<sup>1</sup> International Chamber of Commerce

<sup>2</sup> *Intellectual Property Rights Seizure Statistics: Fiscal Year 2009*, U.S. Customs & Border Protection, Oct 2009

<sup>3</sup> <http://www.livemint.com/2007/06/18001520/Counterfeiters-taking-on-globa.html>



## How Counterfeiting Thrives Online

### Burned by counterfeiters: Zippo Lighters<sup>4</sup>

<b>Revenues:</b>	Zippo lost fully one third of its revenues to counterfeiters between 1995 and 2001.
<b>Employment:</b>	For every 20,000 fake lighters sold, Zippo reduced staff by 1 full-time employee.
<b>Product Safety:</b>	Lower-quality, counterfeit lighters, with a greater tendency to flare up or even explode, caused serious consumer injury.
<b>Liability:</b>	Zippo was named in two lawsuits for incidents involving “Zippo lighters” it had not manufactured.

An entire online supply chain—parallel to legitimate distribution channels—has grown around counterfeit goods. This illicit but highly profitable industry takes advantage of the same online tools, techniques and best practices employed by legitimate brands online.

The contrasts with counterfeiting in the physical world are important to understand, and are founded on the Internet’s global reach, anonymity, and efficiency. These attributes—and especially the online world’s powerful promotional potential—have enabled online counterfeiters to dramatically (and rapidly)

outstrip all the street corner fakes, flea markets and “canal street districts” that exist.

In the wholesale trade, B2B exchanges (also known as trade boards) commonly traffic in counterfeit goods. At the retail level, auction sites and eCommerce sites supply counterfeit goods to consumers. It’s not unusual for individuals to acquire fake goods on wholesale sites, only to resell them to consumers on auction sites and in other online, consumer-facing venues—in addition to offline flea markets, bazaars, and even retail shops.

Promotion is an important part of this illicit ecosystem. Counterfeiters use the same tactics as legitimate marketers, such as paid search ads and search engine optimization to lure buyers to their sites. According to *Direct Magazine*, fully 14 percent of searches on a branded item lead online users somewhere other than the legitimate brand’s site: While some of these searches may lead to legitimate resellers or partners, it’s reasonable to assume that many of them end up on the site of a counterfeiter.

Some counterfeit sellers also employ unsolicited email—spam—to boost their site traffic. This is especially prevalent among sellers of fake pharmaceuticals, software, and luxury goods such as watches, jewelry, and high-end apparel. They also make use of cybersquatting techniques, using branded terms in domain names in order to attract web traffic and convey authenticity. And, as savvy marketers, they take advantage of inbound linking strategies and other search engine optimization (SEO) techniques to sell their illicit goods online.

<sup>4</sup> [http://www.zippo.com/NewsAndEvents/Counterfeiting\\_of\\_Zippo\\_lighters\\_in\\_China\\_affecting\\_Bradford.aspx?article=9209ee4c-ff1e-4712-b340-7f24bf485164&bhcp=1](http://www.zippo.com/NewsAndEvents/Counterfeiting_of_Zippo_lighters_in_China_affecting_Bradford.aspx?article=9209ee4c-ff1e-4712-b340-7f24bf485164&bhcp=1)

The counterfeiting ecosystem extends to popular auction and exchange sites, of course, where direct searches frequently include counterfeit goods among their results. Links to sites pushing counterfeit wares can also be found in quantity on social media venues such as social networking sites, blogs and micro-blogs.

Clearly, legitimate and counterfeit ecosystems overlap—with some auction and eCommerce sites selling both real and fake goods—and this makes the problem more difficult to address. There are best practices, however, which can help brands minimize the damage from online counterfeit sales.

## Beating Back Counterfeiters Online: Seven Best Practices

While the sale of counterfeit goods in the physical world is a timeworn tradition—if an unwelcome one—the online counterfeiting ecosystem offers unique challenges that require a unique online approach. Proven best practices have emerged from brands that have actively and successfully engaged in combating counterfeit sales online.

**1. Attain global visibility.** Before a brand can understand the scope of the threat posed by online counterfeit sales, it must expose and quantify the problem. As we have seen, counterfeiters operate over a wide array of online channels; all of these, including B2B exchanges, auction sites, eCommerce sites, message boards, and the rest, must be monitored and analyzed. There's some good news: just ten online marketplaces account for fully 80 percent of all marketplace traffic. Monitor these marketplaces, and you're watching a significant share of traffic.

The counterfeit sales volumes involved cited here—along with everything else about the Internet—are all enabled by technology. The only possible way to approach the monitoring challenge is to leverage technology as well; there is simply no other practical method.

**2. Monitor points of promotion.** While it's obviously important to identify and shut down distribution channels, it's almost certain that counterfeiters will regularly seek new sales venues. So it's just as critical to monitor the online promotional activities these criminals launch.

Counterfeiters use the same effective promotion techniques employed by legitimate marketers—leveraging the powerful, highly recognizable brands built by experts. Using paid search advertising, links within social media, black hat SEO tactics, cybersquatting and spam, they successfully steer traffic to their illicit offerings, while diminishing the marketing ROI of legitimate brand holders.

Monitoring for these promotional efforts is critical—and enables our next best practice.

### The best tools for fighting technology-enabled counterfeit sales.

<b>Brand:</b>	Snap-on Tools
<b>Challenge:</b>	Significant online sales of counterfeit Snap-on tools, resulted in erosion of revenues, perceived brand value, and customer loyalty.
<b>Response:</b>	Snap-on employed sophisticated monitoring and detection technology solutions to fight online counterfeit sales.
<b>Results:</b>	Counterfeit products valued at \$1.2 million—found in 4,900 illegal auction listings—were identified and removed in coordination with an online auction site.

**3. Take proactive action.** Counterfeiters obviously encounter more success when left to operate unchallenged; they're also known to shift their energies to more passive targets when brands visibly fight back. Once a brand understands where the greatest threats lie, aggressive action is the best strategy. Brands should:

- **Set priorities.** The biggest offenders, offering the greatest number of counterfeit goods in the most highly trafficked venues, should be identified and addressed first. Brand owners should determine which counterfeit goods are generating the largest sales, and target them first as well.
- **Watch for cybersquatters.** Brands should actively monitor cyberspace for unauthorized use of their branded terms in domain names. This will aid in rapid detection of eCommerce sites selling counterfeit or unauthorized goods—and frequently also uncovers other abuses such as false association with offensive content like pornography.
- **Become a difficult target.** Brands that visibly, vigorously fight to remove counterfeit goods from online venues often see a dramatic drop in infringement against their brands.
- **Use all your weapons.** Most online channels provide mechanisms for dealing with counterfeit sales situations. Online marketplaces, for example, typically have policies and procedures enabling brand owners to report listings that infringe their brand. Others often respond readily to emailed complaints from brand owners.  
  
Search engines offer similar facilities. Major search engines have procedures for requesting the removal of ads linked to counterfeit sites. Websites can also be removed from search results pages if they are found to violate copyright laws (a common practice among counterfeit sites, typically through unauthorized use of product images).  
  
Another useful tactic is the sending of takedown notices, which can be sent directly to Internet service providers. In one recent court case<sup>5</sup>, two web-hosting companies were fined \$32 million for not responding to takedown notices aimed at blocking counterfeit sales on sites they hosted.
- **Get help from friends.** Industry relationships can be powerful weapons in the fight against online counterfeiting. When choosing a brand protection solution provider, look for one with established ties with thousands of ISPs

<sup>5</sup> Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc. et al. ; [http://www.ft.com/cms/s/0/54c5a3a4-9686-11de-84d1-00144feabdc0.html?catid=57&SID=google&nclink\\_check=1](http://www.ft.com/cms/s/0/54c5a3a4-9686-11de-84d1-00144feabdc0.html?catid=57&SID=google&nclink_check=1)

and registrars worldwide. Simply put, these ties make it possible to get counterfeit sites shut down more quickly—and thereby minimize brand owner losses. Trade associations such as the International AntiCounterfeiting Coalition (IACC), the Anti-Counterfeiting Group (ACG) and the American Apparel and Footwear Association (AAFA) also provide resources and advice on best practices for fighting counterfeiters.

**4. Fight online counterfeit sales holistically.** Online counterfeit sales are easier to address when the entire enterprise participates. That means brand owners should set up a cross-functional task force to address the issue in a coordinated, holistic manner.

Stakeholders—and, therefore, recommended participants—will vary by industry and enterprise, but can include legal, marketing, risk management, loss prevention, channel sales management, manufacturing, supply chain management, and other functional units.

Because fighting online counterfeiting requires attacking both promotional mechanisms and distribution channels, this group will be larger than needed to fight physical-world counterfeiting. All of these groups can and should set priorities and strategy for detecting, reporting and responding to infringers—both online and off—and should continue to inform the process as their situations and perceptions dictate.

**5. Let online intelligence inform offline defense measures.** Because offline measures—physical investigations, factory raids and other activities—can be costly and time-consuming, it's critical to know where they should be focused. Online intelligence can help identify the most egregious infringers, so that offline defensive efforts can be focused where they'll be most effective.

**6. Act swiftly—and globally.** Perhaps even more than it affects legitimate business, the proliferation of international trade offers tremendous benefits to online counterfeiters. While a domestic seller or manufacturer may seem like an easy first target, brands have learned that it's more effective to launch global anti-counterfeiting initiatives—and to get them underway expeditiously.

#### Footwear manufacturer stomps online counterfeiters.

Global footwear leader Deckers Outdoor, faced with millions in online sales of counterfeit and grey market goods, moved promptly to protect its customers and its bottom line. Leveraging brand protection technology, the company was able to:

- Pinpoint—and remove or de-list—\$4.35 million in illegitimate goods and knock-offs, all within just 90 days
- Significantly curtail counterfeiting activity that undermined its revenues
- Enhance its brand reputation and increase customer trust and loyalty by automating and extending online enforcement

#### Online intelligence helps focus physical efforts.

Acushnet Company, a leader in the golf industry, leveraged online intelligence to guide a major raid in the UK, shutting down a large counterfeiting operation that fed online distribution channels.<sup>6</sup>

<sup>6</sup> CNN: <http://edition.cnn.com/2009/SPORT/09/23/golf.ebay.clubs.scam>

Prepare by ensuring your trademarks are registered internationally—especially in China, which observes a “first-to-file” policy that grants registration to whoever files first, even if it’s not the true brand owner.

### Global imaging giant protects its image—and profits.

Print technology leader Epson created a centralized mechanism for globally monitoring for online brand abuses including counterfeit sales.

By forming a global, cross-functional team, Epson achieved a three-fold reduction in counterfeit sales activities on consumer auction and B2B exchange sites. Their visible, aggressive strategy has also served to deter abuse.

### Tall order: fighting counterfeiting in China.

One of the most important centers of counterfeit trade is China. In addition to originating roughly 89% of counterfeit manufactured goods, China hosts vast internal marketplaces—both online and off—where counterfeit goods are traded.

A global effort doesn’t preclude addressing markets that are internal to a given country. In some cases, this will require competent language translation resources for monitoring, detection and enforcement. Most companies rely on third-party brand protection solution providers for this kind of expertise.

Many online B2B exchanges and auctions are presented only in Chinese-language characters, posing translation barriers to legitimate brands aiming to protect their rights. Regardless of the source of counterfeit goods sold on these sites, buyers commonly re-sell the illicit products in other online and offline venues. Losses to legitimate brands are in the billions.

**7. Educate your customers.** Your customers can be an important ally in minimizing sales of

counterfeit goods with all its associated costs. Work aggressively to show customers the risks of buying from unauthorized sources, and recruit them to join in the effort by reporting suspicious goods and sellers.

Many brands have established web-based tools for verifying the authenticity of goods and/or the legitimacy of sellers. Others provide form- or email-based mechanisms for reporting suspected infringement. When offering such tools, be sure to reinforce the benefits of buying authentic goods from authorized sellers.

Another effective, pro-active measure enables brands to warn consumers directly of known counterfeiting activity, before the consumer makes a purchase. This patented technology leverages relationships with major Internet security providers to deliver early warnings to Internet users, waving them off before they click through to a site known to traffic in counterfeit or recalled goods.

Many consumers don’t want cheap knock-offs—and they don’t want their authentic goods cheapened by the presence of illicit goods. Take advantage of these sentiments: join forces with your customers to spot counterfeit products quickly and help get them off the market.

## Conclusion: The Fight Is Yours to Win

Online counterfeiting can heavily impact any company, affecting revenues, channel relationships, customer experience, marketing effectiveness, legal liability and more. Ignoring it—or just hoping for the best—simply isn't good business.

Fortunately, taking action can be fairly straightforward. Implementing the best practices discussed here doesn't have to involve complex organizational changes or extensive hiring efforts, as third-party solution providers can help make the effort efficient and supplement internal teams.

To successfully reduce the negative effects of counterfeiting, however, companies must commit to forming a cross-functional team, at least at the advisory level, and to an aggressive, global anti-counterfeiting initiative.

Most importantly: to effectively choke off counterfeit sales, these teams must ensure a strategy that focuses on both distribution and promotional mechanisms associated with counterfeit goods. The returns—in revenues, profits, and long-term brand value—will certainly make the effort worthwhile.



## About MarkMonitor

As the global leader in online brand protection, MarkMonitor provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of industry-leading expertise, advanced technology and extensive industry relationships to preserve their marketing investments, revenues and customer trust.

To learn more about MarkMonitor, our solutions and services, please visit [markmonitor.com](http://markmonitor.com) or call us at **1-800-745-9229**.

More than half the Fortune  
100 trust MarkMonitor to  
protect their brands online.  
**See what we can do for you.**

MarkMonitor, Inc.  
U.S. (800) 745.9229  
Europe +44 (0) 203.206.2220  
[www.markmonitor.com](http://www.markmonitor.com)